IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

LUX GLOBAL LABEL COMPANY, LLC Plaintiff, vs. JAMES H. SHACKLETT, IV, et al., Defendants.	CASE NO. 2:18CV05061 Judge C. Darnell Jones, II Magistrate Judge Lynne Sitarski **PLAINTIFF'S REPLY BRIEF IN SUPPORT OF ITS' MOTION TO COMPEL PRODUCTION OF FORENSIC IMAGES AND OTHER SOURCES OF ESI *INSTANTER* [Related Doc. ECF No. 69]**

Plaintiff Lux Global Label Company, LLC ("Plaintiff" or "Lux"), by and through counsel, submits this Reply Brief in support of its February 10, 2020 Motion to Compel Defendants James H. Shacklett. IV ("Shacklett"), CCL Industries, Inc. ("CCL Industries") and CCL Tube (Wilkes Barre) Inc. ("CCL Tube") (collectively referred to as "CCL") to produce the forensic images and data for the following devices and accounts used by Shacklett:

1. Forensic image of Defendant Shacklett's replacement CCL-issued laptop provided to Shacklett on February 23, 2018 ("Shacklett's current CCL-issued laptop");

2. Forensic image of Defendant Shacklett's CCL-issued cell phone allegedly quarantined in 2018 ("Shacklett's cell phone");

3. Forensic image of Defendant Shacklett's iTunes/iCloud account; and

4. Mirror image of Defendant Shacklett's personal email accounts (jshacklett@hotmail.com and jshacklett5@gmail.com) including all sent, received, spam and deleted folders.

[ECF 69].

On February 20, 2020, Plaintiff advised the Court that imaging of Shacklett's quarantined CCL-issued computer was underway, but that Plaintiff's Motion remains pending with respect to

the other remaining Shacklett devices and accounts. [ECF 73]. A Revised Proposed Order granting Plaintiff's Motion to Compel is attached. On February 24, 2020, Defendants filed an opposition to Plaintiff's Motion to Compel and asked the Court to adopt the Delaware Protocol with respect to all remaining electronically stored information ("ESI"), including Shacklett's devices and accounts that contain and were used to access and store Plaintiff's confidential information, wrongfully taken, retained and used by Defendants. [ECF 75]. Throughout Defendants' Opposition, Defendants trumpet their alleged "good faith" willingness to allow images of the thumb drive, Lux's laptop, and Shacklett's quarantined computer. [ECF 75, p. 2]. However, Defendants fail to acknowledge the extraordinary and expensive steps (and Court processes) that Plaintiff was forced to engage in to facilitate Defendants' production of anything or even acknowledgement that they had Plaintiff's information:

1. For months, prior to the filing of any lawsuit, Plaintiff demanded return of its information from Shacklett and CCL. Defendants refused to search for or return anything, ignored Plaintiff's request, and instead accessed and used Plaintiff's information for their benefit.

2. In January 2018, Plaintiff was forced to file a lawsuit to even obtain Defendants' acknowledgement that they had anything belonging to Plaintiff. [*Lux Global Label Co. v. Shacklett, et al* N.D. Ohio Case No. 1:18CV00138, ECF 1].

3. After being caught with Plaintiff's information, Defendants still did not agree to provide anything. The Ohio court had to order Defendants to provide an image of the thumb drive containing Plaintiff's information. [N.D. Ohio ECF 21 Court Order Dated 2/7/2018].

4. Plaintiff voluntarily created its own image of Shacklett's Lux computer without any request from Defendants and willingly turned over the entire image and details to Defendants' expert without any disagreement, Court order, or motion practice.

5. Plaintiff first initiated conversations about imaging Shacklett's devices and accounts in this action when permitted to do so in October 2019. Plaintiff tried to negotiate an acceptable resolution, but when it became apparent that Defendants were unwilling to provide images of Shacklett's accounts and devices, Plaintiff was forced to file a Motion to Compel on February 10, 2020. [ECF 69].

6. After Plaintiff filed a Motion to Compel, Defendants, for the first time, in a conversation with Court on February 18, 2020, stated their willingness to turn over Shacklett's quarantined CCL-issued computer without requiring Plaintiff to waive its rights with respect to Shacklett's other accounts and devices.

Now, Defendants argue that the Delaware Protocol should be adopted for all remaining ESI, including Shacklett's remaining personal email and iTunes/iCloud accounts, cellphone and current CCL-issued computer. For the reasons discussed below, Defendants' proposal is not sufficient or supported by the facts or law under these circumstances.

A. THE DELAWARE PROTOCOL DOES NOT PROVIDE PLAINTIFF WITH SUFFICIENT AND NECESSARY DISCOVERY

The evidence so far obtained demonstrates that Defendants misappropriated Plaintiff's trade secrets. Specifically, Shacklett took Plaintiff's information and attempted to delete the information that he took from Plaintiff's computer as was on the way out the door. Shacklett testified to having used his cell phone and contacts within his iTunes/iCloud accounts to contact Plaintiff's "top performers" for purposes of coming to work at CCL. [Shacklett Dep. 99-103; 136-137]. Despite these damaging facts, Defendants continue to argue their innocence, stating that Shacklett regularly "backed-up" his computer on thumb drives for years[1] [ECF 75, p. 3]; that Shacklett's possession of Plaintiff's information was legitimate due to his travel [Id.]; that none of the information that Shacklett took (and used) was a trade secret [Id.]; and that "neither Shacklett nor CCL used any thumb drive information to compete with or harm Lux." [Id.]. While Defendants make these unsupported and self-serving conclusions, Defendants refuse to provide the very information from which they could support (or Plaintiff could refute) these alleged defenses.

[1] Despite having multiple thumb drives containing Plaintiff's information for many years, Shacklett never mentioned these thumb drives and his apparent continued possession of Plaintiff's information despite multiple requests from Plaintiff. To this day, Shacklett has not provided or disclosed exactly how many thumb drives exist, where they are, or what information belonging to Plaintiff they contain.

The purpose of discovery in this case is two-fold: (1) to obtain relevant discovery; and (2) to facilitate the long overdue return of Plaintiff's information. The forensic image process proposed by Plaintiff is limited to Shacklett's devices and personal accounts that contain Plaintiff's information. The process further limits the discovery from those accounts and devices to information that is either Plaintiff's or relevant to the claims in this case.

Unlike the process proposed by Plaintiff for Shacklett's accounts and devices, the Delaware Protocol allows parties to self-identify and self-search for responsive information. The Delaware Protocol **does not** provide any mechanism to ensure that the most relevant pieces of discovery – Shacklett's devices and accounts – are preserved at any point in time.[2] Instead, under the Delaware Protocol, items in Shacklett's current CCL-issued computer, his personal email accounts, cell phone and iTunes/iCloud accounts are subject to modification, alteration, and destruction by Defendants. Equally troubling, under the Delaware Protocol, Plaintiff is afforded no mechanism to determine how and where Defendants stored, used, modified, transferred, moved, or copied Plaintiff's information.

Defendants disingenuously argue that they are in the best position to search and provide responsive discovery from all devices and accounts. The Delaware Protocol's process, however, is not adequate to ensure the integrity of the information at issue. The nucleus of Plaintiff's misappropriated information is located in Shacklett's accounts and devices – areas that Shacklett has the unfettered ability to move, change, alter, modify, delete or destroy. Contrary to Defendants' assertions, Plaintiff is in the better position to identify its own information and should be permitted the opportunity to do so.

[2] Glaringly absent from Defendants' Opposition are any references to steps that Defendants have taken to preserve any of Shacklett's devices and accounts necessary to prevent spoliation of evidence.

B. DEFENDANTS' ALLEGED CONCERNS OVER CONFIDENTIALITY AND PRIVACY ARE ADDRESSED IN THE PROPOSED PROTOCOL AND THE COURT'S STIPULATED PROTECTIVE ORDER

Defendants argue that the process proposed by Plaintiff is overly invasive and would result in "strangers having direct access to Shacklett's private and personal information and CCL business information that is wholly unrelated to the case, and risks the exposure of privileged information." [ECF 75, p. 1]. In making their argument, Defendants ignore the protections that the protocol contains, as well as, this Court's Stipulated Protective Order. [Id.]. These are the greater protections than Plaintiff has been afforded over its confidential, proprietary and trade secret information that Defendants misappropriated. Defendants fail to identify any reason the Court's protective order is not sufficient to protect its information.

As discussed in detail on page 9 of Plaintiff's Brief in Support, to prove its claims, Plaintiff has to demonstrate that its information exists on Defendants' systems, devices and accounts. The only way to do that is to have access to the relevant sources of data, which in this case are Shacklett's work-related and personal devices and accounts. If Defendants did nothing wrong, as they contend, then they should be willing, and even welcoming the opportunity for Plaintiff to review the data and information at issue.

Courts have routinely found that confidentiality orders are sufficient to protect a competitor's confidential information. *See Robotic Parking v. City of Hobokon*, 2010 U.S. Dist. LEXIS 4575 (N.J. Dist. Jan. 15, 2010); *Balboa Threadworks, Inc. v. Stucky*, 2006 U.S. Dist. LEXIS 29265 *14 (D.Kan. Mar. 24, 2006) (confidentiality over information that is not relevant can be protected through both the terms of the protective order and the search protocol to be used in searching the mirror image).

C. DEFENDANTS' CITATIONS TO DISTINGUISHABLE CASES ARE NOT PERSAUSIVE

Throughout Defendants' Opposition, Defendants cite to a number of cases in an attempt to support their position that Plaintiff is not entitled obtain forensic image and analysis of Shacklett's computer, cell phone and email accounts. [ECF 75, p. 5-8]. However, none of the cases cited by Defendants involve claims of trade secret misappropriation or evidence of Defendants' improper possession, use and access to a competitor's confidential, proprietary, or trade secret information. See *Bianco v. GMAC Mortgage*, 2008 U.S. Dist. LEXIS 84950 (E.D. Pa. Oct. 22, 2008) (a discrimination and retaliation case where plaintiff requested a forensic inspection simply to retrieve requested documents); *Lawson v. Love's Travel Stops & Country Stores, Inc.*, 2019 U.S. Dist. LEXIS 188853 (M.D. Pa. Oct. 31, 2019) (an FLSA case alleging misclassification where defendants were dissatisfied with plaintiffs' ESI production and were requesting that plaintiffs hire an e-discovery vendor); *Hyles v. New York City* 2016 U.S. Dist. LEXIS 100390 (S.D.N.Y. Aug. 1, 2016) (a discrimination and hostile work environment case where the parties were asking the Court to establish rules with respect to ordinary search and production of ESI); *Diepenhorst v. City of Battle Creek* 2006 U.S. Dist.LEXIS 48551 (W.D. Mich. June 30, 2006) (a sexual harassment case where the parties were requesting ordinary discovery and there was no evidence of discovery misconduct or failures); *John B. v. Goetz*, 531 F.3d 448 (6th Cir. 2008) (a class-action case involving Tennessee's managed care system where the district court over-broadly required the images of over 50 state custodians' work and personal devices).

This is not a case like the ones cited by Defendants. Here, the established facts are that Shacklett took Plaintiff's confidential and trade secret information on a thumb drive, in his cell phone and iTunes/iCloud and email accounts, attempted to delete Plaintiff's information and

thereafter, accessed and used Plaintiff's information for the benefit of CCL, Plaintiff's competitor. Although the Defendants would like to ignore it, the facts in the *Stream Cos. v. Winward Adver.*, 2013 U.S. Dist. LEXIS 20200324 (E.D. Pa. Feb. 7, 2013) case cited by Plaintiff are directly on point to the claims here.[3] In *Stream Cos*., as here, a computer expert verified that Shacklett took Plaintiff's confidential information on a thumb drive and attempted to delete Plaintiff's information as he was leaving employment with Plaintiff. Under circumstances similar to these, courts have found that forensic images and analysis are "justified in cases involving both trade secrets and electronic evidence, and granted permission to obtain mirror images of the computer equipment which may contain electronic data related to the alleged violation." See *Ameriwood Indus. v. Liberman*, 2006 U.S. Dist. 93380 *8 (E.D. Miss., Dec. 27, 2006) (forensic images allowed when plaintiff claimed breach of fiduciary duty, misappropriation of trade secrets, unfair competition, tortious interference and conspiracy against former employees who took plaintiff's confidential business files to divert business), quoting *Balboa Threadworks, Inc.* at *8-9 (forensic images allowed when plaintiff accused defendant of copying digital embroidery designs and then selling them); *Cenveo Corp. v. Slater*, 2007 U.D. Dist. LEXIS 8281 (E.D. Pa. Jan. 31, 2007) (forensic images allowed when plaintiff alleged that its former employees improperly used plaintiff's computers and confidential information and trade secrets to divert business from plaintiff to defendants). The facts of this case more closely align with the circumstances in *Stream Co.*, *Ameriwood Indus.,* and *Cenveo*, where the courts allowed forensic imaging when the claims alleged misappropriation of a trade secrets.

[3] While there was evidence of Defendants' subsequent discovery misconduct and refusal to comply with the Court's orders, the Court's initial order at the preliminary injunction stage, required Defendants to produce forensic images of all personal and work-related electronic devices and emails.

D. DEFENDANTS' NARROW VIEW OF THE FACTS AND ALLEGED AND UNVERIFIED EXPENSE DOES NOT PREVENT DISCOVERY.

In a self-serving attempt to narrow the scope of discovery, Defendants argue that the only items subject to forensic discovery are those which "accessed the thumb drive," and therefore there is no need to image Shacklett's cell phone, personal email and iTunes/iCloud accounts. [ECF 75, p. 2, 4, 10]. However, the issue in this case is not just "accessing the thumb drive." Shacklett testified that he downloaded, accessed, and used Plaintiff's information from the thumb drive. [Shacklett Dep. 77; 86-94; 278-280]. Plaintiff is entitled to know what he did with that information, did he modify it, destroy it, transfer it, copy it, email it, store it, or disclose it. Moreover, Shacklett testified that he accessed and used information stored on his cell phone and iTunes/iCloud accounts, when he contacted Plaintiff's "top performers." [Shacklett Dep. 99-103; 136-137]. Finally, Plaintiff is entitled to test the veracity of Defendants' self-serving claims that they have not used Plaintiff's information and have done nothing wrong.

Without any evidence or verifiable facts, Defendants allege that the forensic imaging and analysis that Plaintiff requests would cost Defendants upwards of $20,000. However, Defendants provide no facts, estimates or other data from which the Court can even evaluate Defendants' alleged burden. In fact, the cost of imaging and creating the requested reports for Shacklett's quarantined CCL-issued laptop was less than $2,000, with the actual forensic image costing only $500. [Ex. 1, Invoice for Image]. Moreover, Plaintiff should not be prejudiced due to Defendants' own failures and refusals to return Plaintiff's information and the effects that such refusals and delays have caused them. Despite receiving notice and multiple opportunities to do so, Defendants decided to withhold and not return Plaintiff's information since 2017, forcing Plaintiff to engage in lengthy and costly court processes to obtain return of its own information.

Defendants' alleged burden and expense is of its own making and should not be used to prejudice Plaintiff from pursuing its claims and obtaining return of its information.

For the reasons stated here and in Plaintiff's Motion to Compel [ECF 69], Plaintiff asks that the Court compel the requested forensic images and production in accordance with the Proposed Order attached to Plaintiff's Motion to Compel. [ECF 69-2 to 69-4].

Dated: March 3, 2020

Respectfully submitted,

ZASHIN & RICH CO., L.P.A.

/s/ Ami J. Patel
Stephen S. Zashin (OH #0064557)*
Michele L. Jakubs (OH#0071037)*
Ami J. Patel (OH #0078201)*
950 Main Avenue, 4th Floor
Cleveland, Ohio 44113
Phone: (216) 696-4441
Fax: (216) 696-1618
ssz@zrlaw.com
mlj@zrlaw.com
ajp@zrlaw.com
* *admitted pro hac vice*

COZEN O'CONNOR
Jason A. Cabrera (PA 315804)
David Hackett (PA 80365)
1650 Market Street, Suite 2800
Philadelphia, PA 19103
Phone: 215-665-7235
Fax: 215-701-2261
JCabrera@cozen.com; Dhackett@cozen.com
Attorneys for Plaintiff

Attorneys for Plaintiff

PROOF OF SERVICE

I hereby certify that on March 3, 2020, I electronically filed the foregoing ***Plaintiff's Reply Brief in Support of Its Motion to Compel Production of Forensic Images and Other Electronically Stored Information ("ESI").*** All parties will receive service of this filing through the Court's electronic filing system and electronic mail.

Alexander R. Bilus
PA Atty I.D. No. 203680
SAUL EWING, LLP
Centre Square West
1500 Market Street, 38th Floor
Philadelphia, PA 19102-2186
(Alexander.Bilus@saul.com)

and

David B. Cupar (admitted *pro hac vice)*
Matthew J. Cavanagh (admitted *pro hac vice)*
McDonald Hopkins - Cleveland
600 Superior Avenue, E, Ste. 2100
Cleveland, OH 44114
(dcupar@mcdonaldhopkins.com; mcavanagh@mcdonaldhopkins.com)

/s/ Ami J. Patel
Ami J. Patel

One of the Attorneys for Plaintiff